IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

KIMBERLY WEAR, individually and on behalf of all others similarly situated; *Plaintiff*, v. **DOHMAN, AKERLUND & EDDY L.L.C.**, a Nebraska Corporation, *Defendant*.	Case No.: 24-3186 **COMPLAINT-CLASS ACTION** **JURY TRIAL DEMANDED**

PLAINTIFF'S CLASS ACTION COMPLAINT

Plaintiff Kimberly Wear ("Plaintiff") bring this Class Action Complaint against Dohman, Akerlund & Eddy L.L.C., ("DA&E" or "Defendant"), individually and on behalf of all others similarly situated ("Class Members"), and allege, upon personal knowledge as to their own actions and their counsel's investigations, and upon information and belief as to all other matters:

I. INTRODUCTION

1. This class action arises out of the recent data security incident and data breach that was perpetrated against Defendant (the "Data Breach"), which held in its possession certain personally identifiable information ("PII") and protected health information ("PHI") (collectively, the "Private Information") of Plaintiff and other current and former patients of hospitals that Defendant provided auditing services to, the putative class members ("Class"). This Data Breach occurred on or about February 28, 2024.

2. The Private Information compromised in Defendant Dohman, Akerlund & Eddy L.L.C.'s ("DA&E" or "Defendant") Data Breach included certain personal or protected health information of individuals, including Plaintiff. This Private Information included but is not limited

to "full name, address, date of birth, Social security numbers, medical treatment/diagnosis information, dates of service, health insurance provider name, health insurance claim information, and/or treatment cost"[1]

3. The Private Information was "accessed and/or acquired" by cyber-criminals who perpetrated the attack and remains in the hands of those cyber-criminals. According to Defendant's report to the U.S. Department of Health and Human Services Office of Civil Rights, 9,941 or more individuals' Sensitive Data was compromised.[2]

1. Plaintiff brings this class action lawsuit on behalf of herself and those similarly situated to address Defendant's inadequate safeguarding of Class Members' Personal Information that it collected and maintained, and for failing to provide adequate notice to Plaintiff and other Class Members that their information was likely accessed by an unknown third party and precisely what specific type of information was accessed.

2. Defendant maintained the Private Information in a reckless and negligent manner. In particular, the Private Information was maintained on Defendant's computer system and network in a condition vulnerable to cyberattack. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff and Class Members' Personal Information was a known risk to Defendant and thus Defendant was on notice that failing to take steps necessary to secure the Personal Information from those risks left that information in a dangerous condition.

3. Because of the Data Breach, Plaintiff and Class Members suffered ascertainable

[1] Defendant, *Notice of Data Incident* (October 7, 2024), *available at* https://www.daecpa.com/~daecpaco/files/Dohman-HIPAA_Substitute_Notice_new.pdf (last viewed October 15, 2024).

[2] U.S. Department of Health & Human Services Office for Civil Rights, *Cases Currently Under Investigation*, *available at* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last viewed October 15, 2024).

losses in the form of the losses, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack and the substantial and imminent risk of identity theft.

4. By obtaining, collecting, using, and profiting from the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendant admits that the Private Information was obtained by criminals during the Data Breach.

5. The exposed Private Information of Plaintiff and Class Members can-and likely will-be sold on the dark web. Indeed, Plaintiff and Class Members' Private Information has likely already been published on the dark web.

6. Hackers can offer for sale the unencrypted, unredacted Private Information to criminals. Plaintiff and Class Members now face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers—the gold standard for identity thieves.

7. This Private Information was compromised because of Defendant's negligent and/or careless acts and omissions and the failure to protect the Private Information of Plaintiff and Class Members. In addition to Defendant's failure to prevent the Data Breach, after discovering the breach.

8. Plaintiff and Class Members had no idea their Private Information had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their lifetimes.

9. Plaintiff brings this action on behalf of all persons whose Private Information was compromised because of Defendant's failure to: (i) adequately protect the Private Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected Private

Information using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

10. Plaintiff and Class Members have suffered injury because of Defendant's conduct. These injuries include:

(i) lost or diminished value of Private Information;

(ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information;

(iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including, but not limited to, lost time; and

(iv) the continued and exacerbated harm to their Private Information which:

a. remains unencrypted and available for unauthorized third parties to access and abuse; and

b. may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

11. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that the Private Information of Plaintiff and Class Members was safeguarded. Defendant further disregarded their rights by failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures for the encryption of data, even for internal use.

12. Because of the Data Breach, the Private Information of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

13. Accordingly, Plaintiff sue Defendant seeking redress for their unlawful conduct, and asserting claims for: (i) negligence, (ii) negligence *per se*, and (iii) breach of fiduciary duty.

II. PARTIES

14. Plaintiff Kimberly Wear is and at all times mentioned herein was an individual citizen of Nebraska, residing in the city of Hastings.

15. Plaintiff provided Defendant with her sensitive Private Information as a requirement for her treatment with a hospital that Defendant provided financial services to. Plaintiff saw online that her that her sensitive information was part of Defendant's Data Breach, including her "full name, address, date of birth, Social security numbers, medical treatment/diagnosis information, dates of service, health insurance provider name, health insurance claim information, and/or treatment cost"—which is PHI.

16. Plaintiff reasonably expected and understood that Defendant would take, at a minimum, industry standard precautions to protect, maintain, and safeguard her Private Information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to the same. Plaintiff would not have provided her Private Information to Defendant had she known that Defendant would not take reasonable steps to safeguard it.

17. Plaintiff reasonably expected Defendant to destroy her Private Information after her treatment and/or business relationship with Defendant ended and the Private Information ceased to serve any legitimate business purpose.

18. Plaintiff is very careful about sharing her sensitive PII and PHI. She has never knowingly transmitted unencrypted sensitive PII or PHI over the internet or any other unsecured source. Plaintiff also stores any documents containing her sensitive information in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

19. Because of the Data Breach and at the recommendation of Defendant and its Notice to the Maine Attorney General, Plaintiff made reasonable efforts to mitigate the effect of the Data Breach, including, but not limited to, researching the Data Breach, reviewing financial statements, monitoring her credit information, and changing passwords on her various accounts.

20. Plaintiff has spent much time responding to the dangers from the Data Breach and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to work and recreation.

21. Defendant DA&E is a Nebraska-based entity incorporated in Nebraska that provides financial and auditing services for individuals and businesses, such as hospitals in the Aurora area. Defendant's principal place of business is 1117 12th Street, Aurora, Nebraska, 68818. Defendant's Registered Agent is Thomas L. Stevenson at 1117 12th Street, Aurora, Nebraska, 68818.

22. DA&E is sued both directly and vicariously based on respondeat superior liability under state law, as it is responsible for the actions of all its agents and employees performed in the course and scope of their employment and/or agency. All the actions alleged here by agents and employees of DA&E were so performed. Thus, DA&E is liable for the actions of all its employees and agents, named or unnamed, who performed acts at issue in this lawsuit, all of whom were acting in the course and scope of their employment and/or agency. The actions alleged here were undertaken by DA&E by custom and policy of those entities, making it independently liable under federal law.

III. JURISDICTION AND VENUE

23. This court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5,000,000, exclusive of interest and costs. Upon information and belief, the number of class members is 9,941, many of

whom currently have different citizenship from Defendant, including at least nineteen residents of Maine[3] and . Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

24. This Court has general personal jurisdiction over Defendant because it is an entity based and operating in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

25. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) because Defendant maintains its principal place of business within the District of Nebraska and because a substantial part of the acts or omissions giving rise to this action occurred within this District.

IV. FACTUAL ALLEGATIONS

DEFENDANT'S BUSINESS

26. As described on its website, Defendant provides financial, accounting and auditing services to local individuals and businesses, such as local Aurora hospitals.[4]

27. Throughout this Complaint, all Defendant's associated locations will be referred to collectively as "Defendant."

28. In the ordinary course of receiving health care services from a hospital that Defendant provided services to, each citizen or patient must provide (and Plaintiff and Class Members did provide) Defendant with sensitive, personal, and private information, such as their:

- full name;
- address;
- date of birth;
- Social Security number;
- medical treatment/diagnosis information;
- dates of service;
- health insurance provider name;

[3] https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/88507cf9-8cd3-4516-9b5d-abed21f5c4e6.html (last viewed October 16, 2024).

[4] https://www.daecpa.com/about.php (last viewed October 16, 2024).

- health insurance claim information;
- and/or treatment cost.

29. All of Defendant's Health Care customers, such as the Aurora area hospitals at issue, may share patient information with each other for various purposes, as should be disclosed in a HIPAA compliant privacy notice ("Privacy Policy") that Defendant is required to maintain.

30. Upon information and belief, Defendant's customer's HIPAA Privacy Policy is provided to every patient prior to receiving treatment and upon request.

31. Defendant agreed to and undertook legal duties to maintain the protected health and personal information entrusted to it by its customers and safely, confidentially, and in compliance with all applicable laws, including the Health Insurance Portability and Accountability Act ("HIPAA").

32. The patient and customer information held by Defendant in its computer system and network included the Private Information of Plaintiff and Class Members.

THE DATA BREACH

33. A Data Breach occurs when cyber criminals intend to access and steal Private Information that has not been adequately secured by a business entity like Defendant.

34. According to the Notice of Data Incident,[5]

> Dohman, Akerlund & Eddy, LLC ("DA&E") experienced a data security incident that may affect the privacy of certain patient data. DA&E previously provided auditing services for hospitals in the Aurora, NE area.
>
> On February 28, 2024, DA&E detected suspicious activity on its network and immediately began an investigation. The investigation included the assistance of third-party specialists and determined an unknown party accessed certain files within DA&E's network on or about February 28, 2024. DA&E then conducted a comprehensive review of the files at issue to determine whether personal information may have been involved. After a thorough review of the impacted data, on September 26, 2024, it was

[5] https://www.daecpa.com/~daecpaco/files/Dohman-HIPAA_Substitute_Notice_new.pdf -

> determined that some of your personal information was present in the impacted data set.
>
> DA&E's review included the assistance of third-party data review specialists and determined the potentially impacted information included the following types of information related to patients: name, address, date of birth, Social Security number, medical treatment/diagnosis information, dates of service, health insurance provider name, health insurance claim information, and/or treatment cost.

35. The HHS requires "[i]f a breach of unsecured protected health information affects *500 or more individuals*, a covered entity must notify the Secretary of the breach without unreasonable delay and in *no case later than 60 calendar days* from the discovery of the breach."[6] Further, if "the number of individuals affected by a breach is uncertain at the time of submission, the covered entity should provide an estimate," and later provide an addendum or correction to HSS.[7]

36. Defendant cannot claim they were unaware of the HHS notification requirements as they were late in complying with those requirements by notifying HHS on October 7, 2024.

37. Defendant's notice letter to its victims was dated October 2024—over eight after the incident occurred in February 2024.

38. Defendant had obligations created by HIPAA, contract, industry standards, common law, and representations made to Class Members, to keep Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

[6] U.S. Department of Health and Human Services, *Submitting Notice of a Breach to the Secretary* (Feb. 27, 2023) https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html (last viewed October 15, 2024) (emphasis added).
[7] *Id.*

39. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with their obligations to keep such information confidential and secure from unauthorized access.

40. Defendant's data security obligations were particularly important given the substantial increase in Data Breaches in the healthcare industry preceding the date of the breach.

41. In 2023, a record 3,205 data breaches occurred, resulting in around 353,027,892 individuals' information being compromised, a 78% increase from 2022.[8] Of the 2023 recorded data breaches, 809 of them, or 25.00%, were in the medical or healthcare industry.[9] The 809 reported breaches reported in 2023 exposed nearly 56 million sensitive records, compared to only 343 breaches that exposed just over 28 million sensitive records in 2022.[10]

42. Data breaches such as the one experienced by Defendant have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack.

43. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[11]

44. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

---

[8] *See* Identity Theft Resource Center, *2023 Data Breach Report* (January 2024), *available at* https://www.idtheftcenter.org/publication/2023-data-breach-report/ (last visited October 15, 2024).
[9] *Id*.
[10] *Id*. at 11, Fig.3.
[11] Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack, Security Magazine* (Nov. 23, 2020), *available at* https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited October 16, 2024).

DEFENDANT FAILS TO COMPLY WITH FTC GUIDELINES

45. The Federal Trade Commission ("FTC") has promulgated many guides for businesses which show how important it is to implement reasonable data security practices. According to the FTC, the need for data security should shape all business decision-making.

46. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[12] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity suggesting someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[13]

47. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

48. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and

[12] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (2016), *available at* www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited May 21, 2024).
[13] *Id.*

appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions also clarify the measures businesses must take to meet their data security obligations.

49. These FTC enforcement actions include actions against healthcare providers like Defendant. *See, e.g., In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

50. Defendant failed to properly implement basic data security practices.

51. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to employees' and patients' PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

52. Defendant was always fully aware of its obligation to protect the PII and PHI of its employees and patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

DEFENDANT FAILS TO COMPLY WITH INDUSTRY STANDARDS

53. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

54. Several best practices have been identified that a minimum should be implemented by healthcare providers like Defendant, including, but not limited to, educating all employees; using strong passwords; creating multi-layer security, including firewalls, antivirus, and anti-

malware software; encryption, making data unreadable without a key; using multi-factor authentication; protecting backup data; and limiting which employees can access sensitive data.

55. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

56. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including, without limitation, PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

57. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

DEFENDANT'S CONDUCT VIOLATES HIPAA AND REVEALS ITS INSUFFICIENT DATA SECURITY

58. HIPAA requires covered entities such as Defendant to protect against reasonably anticipated threats to the security of sensitive patient health information.

59. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

60. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a) (1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

61. A Data Breach such as the one Defendant experienced, is considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. 164.40.

62. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate they failed to meet mandated by HIPAA regulations.

V. DEFENDANT'S BREACH

63. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and its data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect employees' and patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that vendors with access to Defendant's protected health data employed reasonable security procedures;

e. Failing to ensure the confidentiality and integrity of electronic PHI they created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

f. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

g. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

h. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

i. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

j. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules related to individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

k. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

l. Failing to train all members of Defendant's workforce effectively on the policies and procedures about PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b); and/or

m. Failing to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as they had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 C.F.R. § 164.304, definition of "encryption").

64. As the result of computer systems needing security upgrading, inadequate procedures for handling emails containing ransomware or other malignant computer code, and inadequately trained employees who opened files containing the ransomware virus, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

65. Plaintiff and Class Members now face an increased risk of fraud and identity theft.

DATA BREACHES PUT CONSUMERS AT AN INCREASED RISK OF FRAUD AND IDENTIFY THEFT

66. Data Breaches such as the one experienced by Defendant's employees and patients are especially problematic because of the disruption they cause to the overall daily lives of victims affected by the attack.

67. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[14]

68. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (or an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[15]

69. Identity thieves use stolen personal information such as Social Security numbers for various crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

70. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give

[14] U.S. Government Accountability Office, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), *available at* https://www.gao.gov/new.items/d07737.pdf (last visited May 21, 2024) ("GAO Report").

[15] Federal Trade Commission, *What To Do Right Away* (2024), *available at* https://www.identitytheft.gov/Steps (last visited June 10, 2024).

the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

71. Theft of Private Information is gravely serious. PII/PHI is a valuable property right.[16] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

72. Theft of PHI is also gravely serious: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[17] Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

73. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which studied data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may

[16] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[17] *See* Federal Trade Commission, *Medical Identity Theft*, *available at* http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited October 16, 2024).

> continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

74. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

75. There is a strong probability that all the stolen information has been dumped on the black market or will be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

76. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[18] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

77. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for more credit lines.[19] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[20] Each of these fraudulent activities is difficult to detect. An individual may not know that her or her Social Security Number

[18] Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), *available at* https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited October 16, 2024).
[19] Social Security Administration, *Identity Theft and Your Social Security Number* (2018), *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited May 21, 2024).
[20] *Id* at 4.

was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

78. It is also hard to change or cancel a stolen Social Security number.

79. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[21]

80. This data, as one would expect, demands a much higher price on the black market. The National Association of Healthcare Access Management reports, "[p]ersonal medical data is said to be more than ten times as valuable as credit card information."[22]

81. Medical information is especially valuable to identity thieves. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016—the same as a Facebook account. That pales in comparison with the asking price for medical data, which was selling for $300 and up.[23]

82. In recent years, the medical and financial services industries have experienced disproportionally higher numbers of data theft events than other industries. Defendant therefore

[21] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), available *at* http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited October 16, 2024).

[22] Laurie Zabel, *The Value of Personal Medical Information: Protecting Against Data Breaches*, NAHAM Connections, *available at* https://www.naham.org/page/ConnectionsThe-Value-of-Personal-Medical-Information (last visited October 16, 2024).

[23] Paul Ducklin, *FBI "ransomware warning" for healthcare is a warning for everyone!*, Sophos (Oct. 29, 2020) *available at* https://news.sophos.com/en-us/2020/10/29/fbi-ransomware-warning-for-healthcare-is-a-warning-for-everyone/ (last visited October 16, 2024).

knew or should have known this and strengthened their data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet they failed to properly prepare for that risk.

VI. PLAINTIFF'S EXPERIENCES

83. Plaintiff Kimberly Wear is and at all times mentioned herein was an individual citizen residing in the State of Nebraska, in the city of Hastings.

84. Plaintiff was a patient at a hospital in Hastings, Nebraska and, on information and belief, that hospital, thereafter utilized Defendant to provide auditing and financial services. Plaintiff was required to provide her Private Information in order to receive healthcare services.

85. After Defendant received Plaintiff's Private Information, including PHI, Defendant's data was breached by unauthorized cybercriminals.

86. When Plaintiff saw that her information may have been stolen, Defendant stated that her PII and PHI may have been either accessed and/or acquired by an unauthorized individual including Plaintiff's "full name, address, date of birth, Social security numbers, medical treatment/diagnosis information, dates of service, health insurance provider name, health insurance claim information, and/or treatment cost."

87. Plaintiff is especially alarmed by the amount of stolen or accessed PII and PHI listed on Defendant's notice. Despite Defendant providing that list, she cannot be sure more of her PII or PHI was exfiltrated. Now she checks her bank accounts and credit cards throughout the day each day, spending approximately an hour per week just monitoring accounts because of Defendant's Data Breach.

88. Plaintiff knows that cybercriminals often sell Private Information, and that her PII or PHI could be abused months or even years after a data breach. In this case, the cybercriminals affirmed they posted Plaintiff's PII and PHI publicly.

89. Had Plaintiff been aware that Defendant's computer systems were not secure, she would not have entrusted Defendant with her personal data.

VII. PLAINTIFF'S AND CLASS MEMBERS' DAMAGES

90. To date, Defendant has not adequately compensated Plaintiff and Class Members for the damages they sustained in the Data Breach.

91. Defendant's vague offer of credit monitoring services is wholly inadequate as it fails to sufficiently compensate all victims of the Data Breach, who commonly face multiple years of ongoing identity theft, and it entirely provides no compensation for its unauthorized release and disclosure of Plaintiff's and Class Members' Private Information.

92. Furthermore, Defendant's credit monitoring advice to Plaintiff and Class Members places the burden on Plaintiff and Class Members, rather than on Defendant, to investigate and protect themselves from Defendant's tortious acts resulting in the Data Breach. Rather than automatically enrolling Plaintiff and Class Members in years of credit monitoring services upon discovery of the breach, Defendant sent instructions to Plaintiff and Class Members about actions they can affirmatively take to protect themselves.

93. Plaintiff and Class Members have been damaged by the compromise and exfiltration of their Private Information in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

94. Plaintiff's Private Information was compromised and exfiltrated by cyber-criminals as a direct and proximate result of the Data Breach.

95. Defendant's Notice of Data Security Incident acknowledges that "the hackers claimed to have published the files that they allegedly copied on their blog site."

96. Plaintiff was damaged in that her Private Information is in the hands of cyber criminals.

97. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an actual, present, immediate, and continuing increased risk of harm from fraud and identity theft.

98. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

99. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

100. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

101. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

102. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Many courts have recognized the propriety of loss of value damages in related cases.

103. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

104. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket

expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed because of failed automatic payments that were tied to compromised cards that had to be cancelled; and

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

105. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by implementing security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing personal and financial information is inaccessible online and that access to such data is password-protected.

106. Further, because of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information —which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

107. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

VIII. CLASS ACTION ALLEGATIONS

1. Plaintiff brings this nationwide class action on behalf of himself and on behalf of others similarly situated under Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

2. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> **All persons whose Private Information was compromised because of the February 2024 Data Breach (the "Class").**

108. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; all federal, state, or local governments, including, but not limited to, their departments, agencies, divisions, bureaus, boards, sections, groups, counsels, and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

109. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

110. Numerosity, Fed R. Civ. P. 23(a)(l): Class Members are so Many that joinder of all members is impracticable. The of affected potential class members includes at lease 9,941, as reported by Defendant to HHS.[24]

[24] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last viewed October 16, 2024).

111. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiff and Class Members;

b. Whether Defendant had duties not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had duties not to use the Private Information of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiff and Class Members;

e. When Defendant learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members;

k. Whether Defendant violated the consumer protection statutes invoked herein;

l. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages because of Defendant's wrongful conduct;

m. Whether Plaintiff and Class Members are entitled to restitution because of Defendant's wrongful conduct; and

n. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced because of the Data Breach.

112. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII compromised because of the Data Breach, because of Defendant's misfeasance.

113. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged here apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct toward the Class as a whole, not on facts or law applicable only to Plaintiff.

114. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

115. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged here; it will permit many Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

116. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

117. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

118. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

119. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

120. And Defendant has acted or refused to act on grounds generally applicable to the Classes and thus final injunctive or corresponding declaratory relief for the Class Members is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

121. Likewise, issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members; and

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief because of Defendant's wrongful conduct.

IX. CAUSES OF ACTION

FIRST COUNT
NEGLIGENCE
(On Behalf of Plaintiff and All Class Members)

3. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

4. Defendant required Plaintiff and Class Members to submit non-public personal information to obtain healthcare services.

5. Plaintiff and Class Members entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their Private Information for business purposes only, and not disclose their Private Information to unauthorized third parties.

6. Defendant was aware of the sensitive nature of the Private Information it required Plaintiff and Class Members to submit, and was aware of the harm that Plaintiff and Class Members would suffer if the Private Information were disclosed.

7. Because it was widely known and reported that healthcare providers are a frequent target of data thieves, Defendant was aware of the likelihood that malicious third parties would attempt to access Plaintiff's and Class Members' Private information.

8. By collecting and storing this data in Defendant's computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from foreseeable attempts at data theft.

9. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period and to give prompt notice to those affected in the case of a Data Breach.

10. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

11. Defendant's duty of care to use reasonable security measures arose because of the special relationship that existed between Defendant and its patients, which is recognized by laws and regulations including, but not limited to, HIPAA, as well as common law. Defendant could ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach or data breach.

12. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all the healthcare, dental, and/or medical information at issue constitutes "protected health information" within the meaning of HIPAA.

13. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

14. Defendant's duty to use reasonable care in protecting confidential data arose not only because of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

15. Defendant breached its duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;

d. Failing to destroy Class Members' Private Information after it ceased to serve any legitimate business purpose;

e. Allowing unauthorized access to Class Members' Private Information;

f. Failing to detect timely that Class Members' Private Information had been compromised;

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

h. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

16. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

17. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

18. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

19. Defendant's negligent conduct is ongoing, in that they still hold the Private Information of Plaintiff and Class Members in an unsafe and unsecure manner.

20. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) provide adequate credit monitoring to all Class Members.

SECOND COUNT
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and All Class Members)

21. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

22. Under the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

23. Under HIPAA, 42 U.S.C. § 1302d, et seq., Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' Private Information.

24. Under HIPAA, Defendant had a duty to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." See definition of encryption at 45 C.F.R. § 164.304.

25. Defendant breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act and HIPAA by failing to provide fair, reasonable, or adequate computer

systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

26. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

27. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

28. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that by failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

29. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

THIRD COUNT
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and All Class Members)

30. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

31. Defendant became guardian of Plaintiff's and Class Members' Private Information, creating a special relationship between Defendant and Plaintiff and Class Members.

32. As such, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

33. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant's relationship with its employees and patients, in particular, to keep secure their Private Information.

34. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' Private Information.

35. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

36. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to return or destroy Plaintiff's and Class Members' Private Information after Defendant ceased to have any legitimate business reason to keep the Private Information.

37. Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

38. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to:

a. actual identity theft;

b. the compromise, publication, and/or theft of their Private Information;

c. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information;

d. lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft;

e. the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession;

f. future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the rest of the lives of Plaintiff and Class Members; and

g. the diminished value of Defendant's services they received.

39. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

X. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of themselves and the Class described above seeks the following relief:

a. For an Order certifying this action as a class action under Federal Rule of Civil Procedure 23, defining the Class as requested herein, appointing Plaintiff and their counsel to represent the Class, and finding that Plaintiff are proper representatives of the Class requested herein;

b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein relating to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c. For equitable relief compelling Defendant to use appropriate methods and policies related to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d. Ordering Defendant to pay for not less than ten years of credit monitoring services for Plaintiff and the Class;

e. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

f. For an award of punitive damages, as allowable by law;

g. For an award of attorneys' fees and costs and any other expense, including expert witness fees;

h. Pre- and post-judgment interest on any amounts awarded; and

i. Any other relief that this court may deem just and proper.

XI. JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury and tenders the fee.

Dated: October 17, 2024

Respectfully submitted,

/s/ Joshua Sanford

Joshua Sanford
Arkansas Bar No. 2001037
jsanford@eksm.com
EKSM, LLP
10800 Financial Centre Pkwy, Suite 510
Little Rock, Arkansas 72211
Telephone: (501) 221-0088
Facsimile: (888) 787-2040

Leigh Montgomery*
Texas Bar No. 24052214
lmontgomery@eksm.com
EKSM, LLP
1105 Milford Street
Houston, Texas 77066
Telephone: (888) 350-3931
Facsimile: (888) 276-3455

(* *pro hac vice* forthcoming)

ATTORNEY FOR PLAINTIFF AND THE PUTATIVE CLASS